



CYBERVERSICHERUNG

Cybergefahren im Planungsbüro – ...

Foto: Ken Schluchtmann, diephotodesigner.de

...ein unterschätztes Unternehmensrisiko

Cybersicherheit bei Architekten und Ingenieuren zwischen BIM, Cloud und Projektverantwortung

Die Digitalisierung hat das Arbeiten von Architekten- und Ingenieurbüros grundlegend verändert. Planungsprozesse werden nahezu vollständig digital abgebildet, Projekte ortsunabhängig koordiniert und Daten in Echtzeit mit Bauherren, Fachplanern, ausführenden Unternehmen und Behörden ausgetauscht. Anwendungen wie Building Information Modeling (BIM), cloudbasierte Projektplattformen, digitale Projektakten oder spezialisierte CAD-Systeme sind heute nicht mehr wegzudenken. Sie steigern Effizienz, Transparenz und Qualität – gleichzeitig machen sie die Planungsbüros jedoch in hohem Maße abhängig von funktionierenden IT-Systemen.

Diese Abhängigkeit ist nicht nur technischer, sondern vor allem wirtschaftlicher und haftungsrechtlicher Natur. Wo früher Papierpläne, lokale Datenbestände und persönliche Übergaben dominierten, sind heute zentrale digitale Datenknoten entstanden. Ein IT-Ausfall, ein Datenverlust oder eine gezielte Manipulation kann unmittelbar den Projektfortschritt gefährden, terminliche Verpflichtungen verletzen und rechtliche Auseinandersetzungen nach sich ziehen. Ge-

rade kleine und mittlere Büros mit hoher Projektlast und wenigen Redundanzen spüren diese Verwundbarkeit besonders stark.

Architekten und Ingenieure geraten zunehmend in den Fokus von Cyberkriminellen, weil sie mit besonders wertvollen und sensiblen Informationen arbeiten. Entwurfs- und Ausführungspläne, statische Berechnungen, Kosten- und Terminstrukturen, Vertragsunterlagen sowie personenbezogene Daten von Bauherren oder Nutzern bilden eine attraktiven Angriffsfläche. Hinzu kommt ihre zentrale Rolle im Projektgefüge. Als Koordinatoren zwischen zahlreichen Beteiligten fungieren sie häufig als Drehscheibe für Informationen. Erlangen Angreifer hier Zugriff, eröffnen sich sowohl Möglichkeiten zur Erpressung als auch zur späteren Manipulation von Projekten oder zur Ausweitung des Angriffs auf weitere Beteiligte.

Cloud und BIM: Fortschritt mit geteilter Verantwortung

Cloud-Lösungen und BIM-Plattformen werden in diesem Zusammenhang oft als besonders sicher wahrgenommen. Tatsächlich investieren professionelle Anbieter erheblich in Verschlüsselung, Verfügbarkeit und physische Sicherheit ihrer Rechenzentren. Dennoch entsteht hier häufig ein trügerisches Sicherheitsgefühl. Die Verantwortung für Cybersicherheit ist geteilt: Während der Anbieter die technische Infrastruktur absichert, verbleiben entscheidende Ri-

siken beim nutzenden Büro. Dazu gehören die Vergabe und Pflege von Zugriffsrechten, der Schutz von Zugangsdaten, die Absicherung von Endgeräten, das Verhalten der Mitarbeitenden sowie die sichere Kommunikation außerhalb der Plattformen. In der Praxis entstehen Sicherheitsvorfälle daher deutlich häufiger durch Fehlkonfigurationen, kompromittierte Zugangsdaten oder menschliche Fehler als durch technische Schwächen auf Anbieterseite.

Typische Cyberrisiken im Planungsalltag

Für Architekten und Ingenieure zeigen sich Cybervorfälle in unterschiedlichen Formen:

- **Phishing-Angriffe**, bei denen Mitarbeitende Zugangsdaten preisgeben
- **Manipulierte Planunterlagen**, etwa durch unbemerkte Änderungen in gemeinsam genutzten Dateien
- **Ransomware-Angriffe**, die den Zugriff auf Projekt- und Bürodaten, wie Mail-Systeme, Termine u.v.m. blockieren
- **Systemausfälle**, die laufende Projekte verzögern oder zum Stillstand bringen
- **Datenschutzverletzungen**, etwa durch Fehlversand sensibler Unterlagen

Die Folgen sind häufig gravierender als zunächst angenommen: Projektverzögerungen, Mehrkosten, Haftungsrisiken, Vertrauensverlust bei Auftraggebern – und nicht zuletzt erheblicher interner Aufwand zur Schadensbewältigung.

Was Planungsbüros konkret tun können

Cybersicherheit beginnt nicht bei einzelnen technischen Maßnahmen, sondern bei einem **ganzheitlichen Ansatz**.

Foto: Ken Schluchtmann, diephotodesigner.de



Foto: Ken Schluchtmann, diephotodesigner.de

Foto: Ken Schluchtmann, diephotodesigner.de



Foto: Ken Schluchtmann, diephotodesigner.de



Bewährt haben sich insbesondere folgende Bausteine:

1. Zugriffsschutz und Identitäten absichern

- Starke, individuelle Passwörter
- Einsatz von **Multi-Faktor-Authentifizierung** für Cloud- und BIM-Zugänge
- Klare Rollen- und Rechtekonzepte nach dem „Need-to-know-Prinzip“

2. Endgeräte konsequent schützen

- Aktuelle Betriebssysteme und Software
- Zentrale Update- und Patchprozesse
- Antivirus- und Firewall-Lösungen auf allen Geräten – auch im Homeoffice und auf der Baustelle

3. Verlässliche Backup-Strategien

- Regelmäßige, automatisierte Datensicherungen
- Getrennte Aufbewahrung (offline oder auf getrennten Systemen)
- Regelmäßige Wiederherstellungstests

4. Mitarbeitende sensibilisieren

Technik kann viel leisten – aber sie ersetzt nicht das Sicherheitsbewusstsein im Alltag. Regelmäßige Schulungen helfen, Phishing-Mails zu erkennen, Risiken richtig einzuschätzen und im Ernstfall korrekt zu reagieren.

5. Prozesse dokumentieren und regelmäßig überprüfen

Gerade bei wechselnden Projektstrukturen, dem Einsatz neuer digitaler Werkzeuge oder der Einbindung externer Dienstleister ist es erforderlich, bestehende Sicherheits- und Datenschutzprozesse regelmäßig zu überprüfen und an veränderte Rahmenbedingungen anzupassen. Eine klare Dokumentation von Zuständigkeiten, Abläufen und technischen Schutzmaßnahmen schafft dabei Transparenz und Nachvollziehbarkeit. Ergänzend kann ein strukturierter Notfall- und Reaktionsplan, der typische Angriffsszenarien und konkrete Handlungsabläufe definiert, im Ernstfall entscheidend zur Schadensbegrenzung beitragen und die Handlungsfähigkeit des Büros sichern.

Restrisiko bleibt – auch bei guter Vorbereitung

So konsequent Prävention auch umgesetzt wird:

Eine hundertprozentige Absicherung ist nicht möglich.

Cyberangriffe entwickeln sich dynamisch, menschliche Fehler lassen sich nicht vollständig ausschließen, und auch technische Systeme können ausfallen. Genau hier setzt der Gedanke des **Risikotransfers** an.

Cyberversicherung als sinnvolle Ergänzung

Eine Cyberversicherung ersetzt keine IT-Sicherheitsmaßnahmen – sie **ergänzt** sie dort, wo Prävention an ihre Grenzen stößt.

Für Architekten und Ingenieure relevant sind insbesondere:

- **Kostenübernahme bei IT-Forensik** und Datenwiederherstellung
- Absicherung von **Betriebsunterbrechungen** infolge von Systemausfällen
- Unterstützung bei **Datenschutzverletzungen**
- Zugriff auf **Spezialisten und Krisenhilfe** im Ernstfall

Darüber hinaus bieten moderne Cyberversicherungen häufig **präventive Zusatzleistungen**, etwa Awareness-Schulungen oder technische Sicherheitschecks, die bereits vor einem Schaden zur Risikominimierung beitragen.

Gerade für kleine und mittelgroße Büros kann dies ein entscheidender Vorteil sein, um Sicherheitsniveau und Krisenfähigkeit nachhaltig zu erhöhen.



Autor



Lars Breitenstein

Produktmanagement Underwriting Cyber
HDI Versicherung AG
HDI-Platz 1, 30659 Hannover
lars.breitenstein@hdi.de



Autor



Peter Bertram

Leiter Produktmanagement &
Underwriting Cyber
HDI Versicherung AG
HDI-Platz 1, 30659 Hannover
peter.bertram@hdi.de



Fazit:

Cybersicherheit als Teil professioneller Planung

Digitale Werkzeuge sind aus der Architektur- und Ingenieurpraxis nicht mehr wegzudenken. Mit ihnen wächst jedoch auch die Verantwortung für den Schutz von Daten, Projekten und Auftraggebern. Cybersicherheit ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess auf organisatorischer, technischer und menschlicher Ebene. Dabei gilt gerade in der digitalen Planungspraxis der Grundsatz: Prävention ist besser als Reaktion. Investitionen in präventive Maßnahmen zur Cybersicherheit sind in der Regel deutlich wirksamer und wirtschaftlicher als die spätere Bewältigung eines Schadensfalls.

Wer Prävention ernst nimmt, klare Strukturen schafft und das Restrisiko bewusst absichert, stärkt nicht nur die eigene Widerstandsfähigkeit, sondern auch das Vertrauen von Bauherren und Projektpartnern. In einer zunehmend digitalisierten Planungswelt wird Cybersicherheit damit zu einem integralen Bestandteil professioneller Projektarbeit und verantwortungsvoller Büroführung.

Foto: Ken Schluchtmann, diephotodesigner.de

